BROMLEY EDUCATIONAL TRUST

BROMLEY EDUCATIONAL TRUST

E-Safety Policy

Responsible post holder	Executive Headteacher
Approved by / on	9th March 2016
Next Review	1st September 2016

This policy is part of the Trust's Statutory Safeguarding Policy/ Procedures. Any issues and concerns with online safety must follow the Trust's safeguarding and child protection processes.

Contents

6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video

Appendices (separate documents):

A1: Acceptable Use Agreement (Staff, Volunteers and Governors)

A2: Acceptable Use Agreements (Pupils – adapted for phase)

A3: Acceptable Use Agreement including photo/video permission (Parents)

A4: Protocol for responding to online safety incidents
http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx - handling infringements
http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf - page 23 onwards

A5: Prevent: Radicalisation and Extremism

A6: Data security: Use of IT systems and Data transfer

Search and Confiscation guidance from DfE
https://www.gov.uk/government/publications/searching-screening-and-confiscation

A7: LGFL Filtering Provider Checklist

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the **Bromley Educational Trust** with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist Academy staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole Trust community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other Trust policies].
- Ensure that all members of the Trust community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our Trust community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting – Youth Produced Sexual Imagery

- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of **Bromley Educational Trust** including staff, pupils, volunteers, parents/carers, visitors, community users who have access to and are users of **Bromley Educational Trust** IT systems

Roles and responsibilities

Role	Key Responsibilities
Executive Headteacher/ Heads of School	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • To ensure Trustees are regularly updated on the nature and effectiveness of the schools' arrangements for online safety • To ensure school websites include relevant information.
Designated E-Safety Child Protection Lead	• Lead role in establishing and reviewing the schools' online safety policy/documents • Promote an awareness and commitment to online safety throughout the Trust community • Ensure that online safety education is embedded within the curriculum for all settings • Liaise with school technical staff where appropriate across the Trust • To communicate regularly with SLT, EHT and the designated online safety Trustee to discuss current issues, review incident logs and filtering • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding

Role	Key Responsibilities
	incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Trustee (E Safety)	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the E Safety Policy and review the effectiveness of the policy • To support the schools in encouraging parents and the wider community to become engaged in online safety activities • The role of the E safety Trustee will include a regular review with the Designated E Safety Lead.
ICT Curriculum Leader	• To oversee the delivery of the online safety element across the curriculum
Network Manager/technician	• To report online safety related issues that come to their attention, to the Designated E Safety Lead, SLT and EHT • To manage the schools' computer systems, ensuring - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices • That they keep up to date with the school's e safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of schools technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to Heads of School/ EHT. • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the schools following data handling procedures as relevant

Role	Key Responsibilities
Teachers	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws • To monitor online behaviour in class and report any concerns to appropriate SLT
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction • To report any suspected misuse or problem to the Designated Lead • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology **Exit strategy** • At the end of the period of employment/volunteering to return any equipment or devices loaned by the schools. This will include leaving IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy annually • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the schools' online safety policy covers their actions out of school • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences

Role	Key Responsibilities
Parents/carers	• To read, understand and promote the schools' Pupil Acceptable Use Agreement with their children • to consult with the schools if they have any concerns about their children's use of technology • to support the schools in promoting online safety including the pupils' use of the Internet and the schools' use of photographic and video images
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within schools • to support the schools in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

Communication:

This policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the schools websites
- Policy to be part of school induction pack for new staff
- Regular updates and training on online safety for all staff
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school

Handling Incidents:

- The schools will take all reasonable precautions to ensure online safety
- Staff and pupils are given information about infringements in use and possible sanctions
- Heads of School will act as first point of contact for any incident
- Any suspected online risk or infringement is reported to Designated Lead on that day
- Any concern about staff misuse is always referred directly to the Executive Headteacher, unless the concern is about the Executive Headteacher in which case the compliant is referred to the Chair of Trust and the LADO (Local Authority's Designated Officer).

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding, Anti-Bullying policy, PSHE, ICT policy).

- The e safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the schools. It has been reviewed prior to the year due to changes in Keeping Children Safe in Education September 2016.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Trustees. All amendments to the Trust e safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

The Trust:

- has an online safety education programme as part of the ICT curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- will remind pupils about their responsibilities through the pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensures pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and Trustee training

The Trust:

- makes regular training available to staff regarding e safety issues and the schools' online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

The Trust:

- runs a programme of e safety advice, guidance and training for parents.
- Promotes e safety through website links

3. Expected Conduct and Incident management

Expected conduct

In our Trust, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and use common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional and reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;
- Monitor pupil usage during lessons and report any concerns regarding individual pupil activity or overall accessibility issues to the internet.

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the schools' rules of appropriate use for the whole Trust community are and what sanctions result from misuse.

Incident Management

In our Trust:

- there is strict monitoring and application of the e safety policy and a differentiated and appropriate range of sanctions;
- all members of the schools are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the schools' escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;

- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in online safety within the schools;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

Schools in England (and Wales) are required "*to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*". Furthermore, the Department for Education published the revised statutory guidance 'Keeping Children Safe in Education' 5th September 2016 for schools and colleges in England. Amongst the revisions, schools are obligated to "*ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."
It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision. All Trust Schools operate the LGFL filtering system (see appendix for LGFL Filter Assessment).

The Trust:

- has the educational filtered secure broadband connectivity through the LGfL;
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect pupils.
- informs all users that Internet/email use is monitored; it is the class teacher and any other adult in the room to monitor pupil activity on the internet and report any concerns immediately. Specific staff have access to all accounts, including staff and monitoring is carried out when/ where required.

Network management (user access, backup)

The Trust:

- Uses individual, audited log-ins for all users - the LGfL USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Uses teacher 'remote' management control tools at BTA Hayes Campus for controlling workstations/viewing users' for BTA sites
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school data (admin and curriculum);
- Storage of all data within the schools will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, the schools:

- Ensure staff read and sign that they have understood the schools' online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- All pupils have their own unique username and password which gives them access to the Internet and other services;
- Make clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Have set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Require all users to log off when they have finished working or are leaving the computer unattended;
- Ensure all equipment owned by the schools and/or connected to the networks have up to date virus protection;
- Make clear that staff are responsible for ensuring that any computer or laptop loaned to them by the schools is used primarily to support their professional responsibilities.
- Maintain equipment to ensure Health and Safety is followed;
- Ensure that access to the schools' network resources from remote locations by staff are audited and restricted and access is only through school/LA approved systems:
- Do not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
- Have a clear disaster recovery system in place that includes a secure, remote off site back up of data;

- Use secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Passwords

- The schools make it clear that staff and pupils must always keep their passwords private, must not share with others; if a password is compromised the schools should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staffs are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.

E-mail

The schools

- Provide staff with an email account for their professional use and makes clear personal email should be through a separate account.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.
- Use a number of LGfL-provided technologies to help protect users and systems in the schools, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:

- We use LGfL pupil email system which is intentionally 'anonymised' for pupil protection.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff can only use the LGfL e mail system on the school system.
- Staff will use LGfL e-mail systems for professional purposes.
- Access in school to external personal e mail accounts may be blocked.

School website

- The Executive Headteacher, supported by the Trust Board, takes overall responsibility to ensure that the websites are accurate and the quality of presentation is maintained;
- The school websites complies with statutory DFE requirements;
- Most material on the websites are the schools own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school websites;

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred systems for such communications.
- Any school approved social networking will adhere to schools' communications policy.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil. Any exceptions must be approved by the Executive Headteacher.
- They do not engage in online discussion on personal matters relating to members of the schools community;
- Personal opinions should not be attributed to the school /academy and personal opinions must not compromise the professional role of any staff member, nor bring the Trust into disrepute;
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.
- Breach of any of the above could lead to gross misconduct.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Pupils are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

In this Trust:

- The Executive Headteacher is the Senior Information Risk Officer (SIRO).
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, pupils & parents or visitors own risk. The Schools accept no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- If a pupil brings his or her mobile phone or personally-owned device into school then it will be handed in at the start of the day. If the device is not handed in and found during the day then it will be confiscated.
- Staff mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Executive Headteacher / Heads of School. Staff members may only use their personal phones during school break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at another time than their break times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Executive

Headteacher/ Heads of School. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Executive Headteacher/ Heads of School are able to withdraw or restrict authorisation of use at any time, if it is deemed necessary.

- The Schools reserve the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff school mobile devices may be searched at any time as part of routine monitoring.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office as the phone will be locked away and therefore not answered.

Digital images and video

In our schools:

- We gain parental/carer permission for use of digital photographs or videos involving their child as part of the school agreement form when their daughter/son joins the school;
- We do not identify pupils in online photographic materials;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use;
- The school blocks/filters access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated and are also taught to consider how to publish for a wide range of audiences which might include Trustees, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Appendices

BROMLEY EDUCATIONAL TRUST

Staff, Trustee and Visitor
Acceptable Use Agreement /Code of Conduct

- ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff, Trustees and Visitors are aware of their professional responsibilities when using any form of ICT. All staff, Trustees and Visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head of School or Executive Headteacher.
- I will only use the school's email/ Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Executive Headteacher or Trust Board.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils, and any other stakeholders are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address to pupils.
- I will only use the approved, secure email system for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Executive Headteacher , Head of School or Trust Board.
- I will not install any software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Executive Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Executive Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the Trust community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the Trust's E-Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …… Date ……

Full Name …… (print)

Job Title ……

KS1 Acceptable Use Agreement

Think before you click

S

I will only use the Internet and email with an adult

A

I will only click on icons and links when I know they are safe

F

I will only send friendly and polite messages

E

If I see something I don't like on a screen, I will always tell an adult

My Name:

BROMLEY EDUCATIONAL TRUST

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe:

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*

BROMLEY EDUCATIONAL TRUST

KS3/4 Pupil Acceptable Use Agreement

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's computers for appropriate school activities and learning and am aware that the school can monitor my internet use.
2. I will not bring files into school that can harm the school network or be used to circumvent school security tools
3. I will only edit or delete my own files and not view, or change, other people's files or user areas without their permission.
4. I will keep my logins, IDs and passwords secret and change my password regularly.
5. I will use the Internet responsibly and will not visit web sites that are inappropriate for the school or my key stage.
6. I will only e-mail or contact people I know, or those approved as part of learning activities
7. The messages I send, or information I upload, will always be polite and sensible. All messages I send reflect on me and the school.
8. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file.
9. I will not give my personal information that could be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
11. If I see anything I am unhappy with or I receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.
12. I am aware that some websites, games and social networks have age restrictions and I should respect this.
13. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.

I have read and understand these rules and agree to them.

Signed: *Date:*

BROMLEY EDUCATIONAL TRUST

Data Security

Passwords - Do

- use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers)

Passwords - Don't

- ever share your passwords with anyone else or write your passwords down
- save passwords in web browsers if offered to do so

Laptops - Do

- try to prevent people from watching you enter passwords or view sensitive information
- log-off / lock your 'desktop' when leaving your PC or laptop unattended.

Sending and sharing - Do

- be aware of who you are allowed to share information with. Check with your Information Asset Owner(s) if you are not sure. [The SIRO and IAOs need to ask third parties, (if non LA approved), how they will protect sensitive information once it has been passed to them]
- only use encrypted removable media (such as encrypted USB pen drives) if ever taking any 'Protected' data outside your school.

Sending and sharing - Don't

- send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives), if secure remote access is available.
- send sensitive information by email unless it is encrypted; Pupil data must be sent via S2S (DCSF secure web site)

Working on-site - Do

- lock sensitive information away when left unattended, i.e. in lockable drawers, log off or lock work station

Working on site - Don't

- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room.

Working off-site - Do

- only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above
- wherever possible access data remotely instead of taking it off-site - using approved secure authentication
- make sure you sign out completely from any services you have used
- ensure you save to the appropriate area to enable regular backups

BROMLEY EDUCATIONAL TRUST

London Grid for Learning Provider Checklist

Company / Organisation	London Grid for Learning Known as LGfL, TRUSTnet or LGfL TRUSTnet
Address	LGfL, CI Tower, St George's Square, New Malden, KT3 4TE
Contact details	020 82 555 555 (option 9)
Filtering System	WebScreen™ 2.0 (incorporating NetSweeper and Fortinet technologies)
Date of assessment	17 June 2016

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification	

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
● Are IWF members		WebScreen™ 2.0, the internet filtering solution applied to the LGfL TRUSTnet network, uses URL filtering from NetSweeper and Fortinet, which are both IWF members. Furthermore, LGfL is currently exploring closer partnership working with the IWF.
● and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		The IWF CAIC list is actively implemented by NetSweeper. This is an always-on feature to comply with legislation and ensure safeguarding for school staff and students – it cannot be turned off by schools.
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		This is applied to WebScreen™ 2.0 directly by our support partner Atomwide. This is an always-on feature to comply with legislation and ensure safeguarding for school staff and students – it cannot be turned off by schools.

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		LGfL's WebScreen™ 2.0 filtering product categorises web content into one or more distinct categories (see Appendix 1), which may (or may not, subject to other local or regional legal obligation or precedent) then be blocked or allowed according to the assigned category/ies, individual URL/s, or the policies defined by the school. Websites unequivocally identified as illegal or a network security risk are automatically categorised and blocked. This cannot be changed by a school. Where a website has been established as potentially inappropriate, however, or if it falls into a high-risk or other category which is blocked by default, a school may take an informed decision to allow these sites in one or more policies. This might be to enable discussion of certain themes in lessons, or where a site's appropriateness may depend upon the age and maturity of users.

			A range of appropriate, balanced default policies are available to suit the typically differing requirements of primary and secondary schools, for both staff and students, which local school administrators can then modify, by blocking or allowing further categories, websites and webpages, and even applying different profiles to different times of day, different logins, or different computers (e.g. Facebook for teachers but only after 3pm, YouTube for pupils at lunchtime, etc.). The default policies are there to enable informed and proactive safeguarding decisions. Free training courses are offered to all schools to help them best understand and manage the filtering / policy system and interface. Alternatively, an authorised Nominated Contact can request individual category blocking / unblocking requests via the LGfL Support Site. LGfL also has a dedicated Safeguarding Board which works on reviewing the filtering systems from a purely safeguarding perspective. The Board also develops keyword lists based on the latest best-practice and school experience, to aid with up-to-date school-safe and school-appropriate filtering. These keyword lists are added as a further layer over the Google Safe Search functionality, which is turned on by default for all schools. Google's YouTube service is available in the modes: open, moderate restricted and severe restricted. All LGfL default to 'severe-restricted' mode, which is recommended. However, schools are permitted to change their settings to use YouTube in 'moderate-restricted' mode. Any school wanting to turn off restricted mode altogether is warned that this is highly inadvisable in an education setting – however, with the approval of the Headteacher, they may bypass DNS settings in order to do so. As part of LGfL TRUSTnet's remit to support education in schools, the online-safety portal os.lgfl.net provides a collated and curated portfolio of resources to help teachers, managers, parents and children learn to become effective and safe digital citizens. Many of these resources

			reflect the management of, rather avoidance of risk, in recognition of the dangers of overblocking. Resources are drawn from the entire online-safety community and a variety of providers, but two LGfL resources are particularly relevant in relation to the balancing act of safeguarding vs overblocking: 'Counter-Extremism: narratives and conversations' deals with specific online threats from exposure to extremist material and potential grooming; 'Trust Me' (developed in partnership with Childnet) aims to engender critical-thinking skills in Primary and Secondary pupils about their online experiences (contact, content and propaganda).
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		See above
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		See above
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		See above
Pornography	displays sexual acts or explicit images		See above
Piracy and copyright theft	includes illegal provision of copyrighted material		See above
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		See above
Violence	Displays or promotes the use		See above

	of physical force intended to hurt or kill		

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects.

WebScreen™ 2.0 utilises the strengths of its underlying technology partners, NetSweeper and Fortinet, but then expands those strengths, and regionalises the results, so that they better suit the UK education sector.

To expand on the capabilities described elsewhere in this response, WebScreen™ 2.0 offers:

Extra 'localised' and specialist web site categories not typically found in commercial filtering, and offering better compatibility with schools' needs.

A devolved hierarchy of central/local policies, that can be adopted and then modified by the local establishment to best suit its particular circumstances, or used in their default state for those with no need or desire to localise the filtered experience.

Data Controller authorisation, which is sought for certain 'high risk' categories, in order to ensure that a full awareness exists within (for instance) a school's Senior Leadership Team, of any polices being deployed that may represent a higher risk than is typically deemed acceptable.

Highly granular settings can enable filtering policies to differentiate between such status as staff and students, locations, times of day, the nature of physical and wireless connections, specific devices by type or ID, and can also conveniently accommodate USO account-holding visitors from other establishments, or non-USO account holding 'Guests' via a range of options.

The service is extremely well documented, and transparent (except where negated by legal or other obligation) in its application of site categorisation and policy application, management and governance.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

WebScreen™ 2.0's content categorisation is a continuous ongoing process, supported by NetSweeper global URL lists and automated AI (artificial intelligence), and underpinned by UK-regionalised categorisation obtained using 'crowd-sourced' intelligence from within its own user community.

Local control of policies is actively encouraged, while guidance is provided regarding the need for a balanced approach to filtering being combined with practical and informed support from staff, and the issues that can be encountered by establishments being either too open or too zealous within any given filtering policy.

Where policies are deemed to be effectively appropriate, but needing occasional or temporary exceptions to be applied due to changes in circumstances, WebScreen™ 2.0 policies can be readily modified, and later returned to their otherwise normal state.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
• Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role		WebScreen™ 2.0 default filter policies are applied appropriate to the underlying nature of a filtered establishment (i.e. Primary School, Secondary School, Teachers' Centre, etc.). Per User filtering is available for deployment across all customer establishments. Multiple filtering policies can be applied, in order to recognise the needs of different groups of users, or locations, or times of day, and/or combinations of each of the above. Filtering policies can be tailored to respond accordingly to different groups of identified individual users, or even a single user.
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		Yes, fully configurable by appropriately authorised local establishment contacts, or their contracted support agents, via an online portal available 24x7.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Yes, WebScreen™ 2.0 categorises 121 distinct content categories, with descriptions of the purpose and summarised content of each, and where appropriate, the implications of access, and/or prerequisites for gaining access.

● Identification - the filtering system should have the ability to identify users		WebScreen™ 2.0 is fully integrated with the LGfL Shibboleth-compliant IdP, referred to as Unified Sign On (USO), which is run by support partner Atomwide. The system therefore recognises any user presenting a USO ID in response to a filtering policy generated request.
● Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies		WebScreen™ 2.0 filters any content accessed by http and https protocols, regardless of whether content is browser or application (app) accessible, and is equally applicable to 'mobile' content accessed via an establishment's filtered infrastructure.
● Multiple language support – the ability for the system to manage relevant languages		Yes, via the NetSweeper embedded technology, WebScreen™ 2.0 supports multi-language filtering.
● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		No local installed software, nor additional hardware, is required for client devices connected to an establishment's filtered infrastructure.
● Reporting mechanism – the ability to report inappropriate content for access or blocking		Yes, via the online management portal, the option to suggest global re-categorisation, or request local re-categorisation, of an individual site or URL, is available to appropriately authorised local establishment contacts, or their contracted support agents.

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum*".[3]
Please note below opportunities to support schools (and other settings) in this regard

Free training courses are offered to all schools to help them best understand and manage the filtering / policy system and interface. Alternatively, an authorised Nominated Contact can submit individual category blocking / unblocking requests via the LGfL Support Site.

LGfL also has a dedicated Safeguarding Board which works on reviewing the filtering systems from a purely safeguarding perspective. The Board also develops keyword lists based on the latest best-practice and school experience, to aid with up-to-date school-safe and school-appropriate filtering.

As part of LGfL TRUSTnet's remit to support education in schools, the online-safety portal os.lgfl.net provides a collated and curated portfolio of resources to help teachers, managers, parents and children learn to become effective and safe digital citizens. Many of these resources reflect the management of, rather avoidance of risk, in recognition of the dangers of overblocking.

Resources are drawn from the entire online-safety community and a variety of providers, but two LGfL resources are particularly relevant in relation to the balancing act of safeguarding vs overblocking: 'Counter-Extremism: narratives and conversations' deals with specific online threats from exposure to extremist material and potential grooming; 'Trust Me' (developed in partnership with Childnet) aims to engender critical-thinking skills in Primary and Secondary pupils about their online experiences (contact, content and propaganda).

PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	John Jackson
Position	Chief Executive Officer
Date	20 June 2016